CENTRE FOR
CYBER SECURITY
BELGIUM

Baseline Security Guidelines (BSG)

Résumé destiné à la direction (FR)

CENTRE FOR

CYBER SECURITY BELGIUM

Rue de la Loi, 16 – Brussels

info@ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be

Introduction

La sécurité de l'information s'impose désormais parmi les défis organisationnels que chaque dirigeant doit intégrer. Il s'agit d'un élément essentiel de toute stratégie d'organisation visant à protéger ses ressources essentielles (actifs), afin de garantir au minimum les éléments suivants :

- Récupération (et non perte) de la confiance du client
- Protection de la réputation
- Continuité de l'activité
- Amélioration de la résilience à la cybercriminalité (par exemple, les logiciels de type ransomware et autres logiciels malveillants)
- Résistance en cas de cyberincident

En tant que telles, les données ne valent souvent pas grand-chose, tant qu'elles ne sont pas traitées, organisées, agrégées, manipulées pour en retirer des informations et des connaissances.

L'information est la valeur de base d'une organisation ; elle doit donc être bien protégée par des mesures de sécurité appropriées, qui font partie de la bonne gestion qu'une autorité publique doit mettre en place.

La protection de l'information se complexifie chaque jour un peu plus dans un monde interconnecté.

La sécurité de l'information n'est pas seulement une question technique, elle est également nécessaire pour établir des règles et garantir leur respect.

L'importance de la sécurité de l'information pour les dirigeants

Les avantages d'un système de gestion de la sécurité des informations pour votre organisation sont les suivants :

- Amélioration de la valeur et de la réputation de votre organisation en démontrant un système de gestion efficace
- Réduction des risques et incidents de sécurité
- Protection contre les exigences légales ou réglementaires
- Une structure permettant d'utiliser plus efficacement les investissements informatiques
- Un outil précieux pour répondre aux incidents de cybersécurité majeurs
- Augmentation du niveau de confiance dans le fait que les décisions se fondent sur des données réelles
- Un moyen de démontrer à vos partenaires externes que la sécurité de l'information est prise au sérieux et la leur imposer
- Ils assurent le traitement confidentiel des données

Remarque : La sécurité informatique est bien plus limitée que la gestion de l'information, car elle concerne la partie « automatisée » de la gestion de l'information. La diffusion orale d'informations, de façon informelle, par exemple dans un ascenseur, ne relève pas de la sécurité informatique, mais de la sécurité de l'information.

Pour accompagner la mise en œuvre d'un système de sécurité de l'information, nous avons élaboré ce guide. Les BSG (Baseline Security Guidelines) reposent intégralement sur la norme ISO27001, mais elles se concentrent sur les organismes publics et contiennent une proposition de méthode par étapes.

Les obligations légales relatives à la protection des données à caractère personnel (RGDP) ne sont pas reprises ici, mais sont certainement applicables dans ce domaine spécifique.

Gestion de la sécurité de l'information - 4 principes de base -15 points d'attention

Lors de la définition d'une bonne gestion de la sécurité de l'information, **quatre grands principes de base** doivent être pris en compte :

1. Stratégie de sécurité et soutien
2. Inventaire des actifs et analyse des risques
3. Mise en œuvre des mesures de sécurité
4. Évaluation des mesures de sécurité

Ces principes de base en matière de sécurité de l'information doivent être évalués en continu afin d'améliorer la qualité (le modèle PDCA = "Plan, Do, Check, Act").

Ces quatre principes comportent **15 points d'attention** formulés comme suit :

Stratégie de sécurité et de soutien

1. **L'implication et le soutien de la direction** sont nécessaires pour garantir une stratégie de sécurité et veiller à ce que les structures, les procédures et les ressources opérationnelles y soient associées.
2. Vous élaborez **une stratégie de sécurité de l'information (politique de sécurité)** conforme à la stratégie de l'organisation pour soutenir les objectifs dans le respect des lois et réglementations.
3. Vous élaborez un plan pluriannuel de **formation et de sensibilisation** régulières de tous les collaborateurs internes et externes et de votre organisation dans son ensemble.

4. Vous intégrez dès le départ **une culture de la sécurité de l'information et de l'analyse des risques** pour tous les nouveaux projets, qu'il s'agisse du développement de nouvelles applications ou de projets d'entreprise.
5. Vous disposez d'un plan d'**incidents** et de crises **de sécurité** majeurs/graves.
6. Vous disposez d'un registre des modifications importantes de l'environnement que vous tenez à jour.
7. Vous disposez d'un **plan de continuité de l'activité** (PCE) et d'un plan de reprise après sinistre (**Disaster Recovery Plan (DRP**) d'appui et lié aux aspects informatiques.

Inventaire des actifs et analyse des risques

8. **Vous identifiez les systèmes d'information et les données clés** et leurs propriétaires, puis définissez les rôles et les responsabilités.
9. Vous adoptez, avec l'aide de la direction, une **politique de catégorisation des systèmes d'information sensibles et des données**, fondée sur les principes de confidentialité, d'intégrité et de disponibilité (CIB, en anglais CIA) pour toute la durée de vie. Il s'agit de revoir régulièrement ce point.
10. **Vous gérez les risques en matière de sécurité de l'information** afin de définir des priorités et de prendre les mesures appropriées pour les réduire à un niveau acceptable par l'organisation, de manière à réduire les effets potentiels.

Mise en œuvre des mesures de sécurité

11. Vous mettez en œuvre des **mesures spécifiques (techniques/organisationnelles/processuelles)** pour protéger les informations.
12. **Vous gérez les ressources** allouées à la sécurité et à l'infrastructure de l'information de manière efficace et efficiente, y compris la désignation de fonctionnaires en sécurité de l'information.

4. Évaluation des mesures de sécurité

13. Vous effectuez au moins **une évaluation annuelle des mesures de sécurité** afin de mesurer l'état du plan de sécurité. Les améliorations et les ajouts possibles sont nécessaires pour chaque organisation.
14. **Vous mesurez les performances des actions mises en œuvre** (points précédents), tout en analysant l'évolution des menaces et des vulnérabilités à intervalles réguliers afin de garantir la réalisation des objectifs (cycle d'amélioration continue :PDCA).
15. Vous envisagez **d'affiner l'analyse des risques et les mesures de gestion** à la lumière des évaluations (point 13), des audits, des incidents survenus et des modifications importantes qui ont ou ont eu une incidence sur les activités de l'entreprise.